SPHINCS$^+$

Modifications for update to Round 3 submission to the NIST post-quantum project

Jean-Philippe Aumasson, Daniel J. Bernstein, Ward Beullens,
Christoph Dobraunig, Maria Eichlseder, Scott Fluhrer,
Stefan-Lukas Gazdag, Andreas Hülsing, Panos Kampanakis, Stefan Kölbl,
Tanja Lange, Martin M. Lauridsen, Florian Mendel, Ruben Niederhagen,
Christian Rechberger, Joost Rijneveld, Peter Schwabe, Bas Westerbaan

March 2, 2022

1 Preventing long-message attacks when using SHA256

As announced in the email to pqc-forum on March 17, 2021, we changed the instantiations of $\mathbf{H_{msg}}$ and $\mathbf{PRF_{msg}}$ using SHA2 in Section 7.2.2.

2 Mitigating security degradation under multi-user attacks in key generation

As announced in the email to pqc-forum on January 17, 2022, the **PRF** specification in section 7.2 was updated to prevent multi-user attacks.

We decided to enforce that the address input **ADRS** takes the same position in the input for the fixed input length functions. This achieves domain separation for those functions.

In this context we introduced dedicated address for WOTS$^+$ and FORS key generation which separate the use of **PRF** in these use cases from each other and from other functions. The types are identical to the WOTS$^+$ and FORS address types respectively except that they have a different type word.

3 Mitigating security degradation under multi-user attack in $\mathbf{PRF_{msg}}$

As announced in the email to pqc-forum on January 17, 2022, we changed the initialization of the optional randomness value from the all-zero string to PK.seed. The change can be found in section 6.4. In this step we also updated the respective paragraph in Section 1.1 where we clarified that the randomness is n bytes and not fixed to 256-bits (which is what was already stated in the main body of the specification). We also removed a previous comment saying that the use of true randomness may be helpful to avoid side-channel attacks as even the possibility to contribute to side-channel protection seems debatable.

4 Mitigating multi-target attacks against $\mathbf{T}$ for long inputs

On April 21, 2022, Sydney Antonov pointed out a multi-target attack against the tweakable hash function **T** when instantiated with SHA2-256. The problem is caused by the small internal state of SHA2-256. It concerns the $n = 32$ parameters and in less severity the $n = 24$ parameters. Therefore, we changed the instantiations of **H** and **T** for these parameters to use SHA2-512 in Section 7.2.2.

5 Minor changes

We fixed the following minor points:

- In the official comment on November 2, 2021, we announced a new tight security proof for SPHINCS$^+$. The full paper can now be found on eprint as [1]. The security evaluation section now contains the reference.

- Renamed SHA-256 parameters into SHA2 parameters to express that we are also using SHA2-512. For consistency we also renamed the SHAKE256 parameters into SHAKE parameters.
- Section 6.4, in function `spx_sign`: The input to the call to function `fors_pkFromSig` incorrectly took message `M` instead of the computed message digest `md`. This got corrected
- Section 7.1.1, under "Verification." Added footnote that clarifies that the bound is a worst case bound and that mentions the average case bound which explains actual measurements.
- Section 9, under "Reductionst proof": The sentence above Theorem 9.1 was missing that the theorem talks about $\mathbf{T}$, too. Corrected.
- Extended acknowledgements.

References

[1] Andreas Hülsing and Mikhail Kudinov. Recovering the tight security proof of *sphincs*$^+$. Cryptology ePrint Archive, Report 2022/346, 2022. https://ia.cr/2022/346. 2